

ON RESIDUALLY FINITE SEMIGROUPS OF CELLULAR AUTOMATA

TULLIO CECCHERINI-SILBERSTEIN AND MICHEL COORNAERT

ABSTRACT. We prove that if M is a monoid and A a finite set with more than one element, then the residual finiteness of M is equivalent to that of the monoid consisting of all cellular automata over M with alphabet A .

1. INTRODUCTION

In a concrete category, a *finite object* is an object whose underlying set is finite. A *finiteness condition* is a property relative to the objects of the category that is satisfied by all finite objects. Finiteness is a trivial example of a finiteness condition. Hopficity and co-Hopficity provide examples of finiteness conditions that are non-trivial and worth studying in many concrete categories, e.g., the category of groups, the category of rings, the category of compact Hausdorff spaces, etc. (see the survey paper [12] and the references therein). We recall that an object X in a concrete category \mathcal{C} is called *Hopfian* if every surjective endomorphism of X is injective and *co-Hopfian* if every injective endomorphism of X is surjective. Another interesting finiteness condition is *residual finiteness*. An object X in a concrete category \mathcal{C} is said to be *residually finite* if, given any two distinct elements $x_1, x_2 \in X$, there exists a finite object Y of \mathcal{C} and a \mathcal{C} -morphism $\rho: X \rightarrow Y$ such that $\rho(x_1) \neq \rho(x_2)$.

Suppose now that we are given a monoid M and a finite set A . We say that a map $\tau: A^M \rightarrow A^M$ is a *cellular automaton* over the monoid M and the *alphabet* A if τ is continuous for the prodiscrete topology on A^M and M -equivariant with respect to the shift action of M on A^M (see Section 2 for more details). It is clear from this definition that the set $\text{CA}(M, A)$, consisting of all cellular automata $\tau: A^M \rightarrow A^M$, is a monoid for the composition of maps.

The main result of the present note is the following statement which yields a characterization of residual finiteness for monoids in terms of cellular automata.

Theorem 1.1. *Let M be a monoid and let A be a finite set with more than one element. Then the following conditions are equivalent:*

- (a) *the monoid M is residually finite;*
- (b) *the monoid $\text{CA}(M, A)$ is residually finite.*

Date: August 20, 2015.

2010 Mathematics Subject Classification. 20E26, 20M30, 37B10, 37B15, 68Q80.

Key words and phrases. cellular automaton, monoid, semigroup, residual finiteness, Hopficity.

Residual finiteness is obviously hereditary, in the sense that every subobject of a residually finite object is itself residually finite. Thus, an immediate consequence of implication (a) \Rightarrow (b) in Theorem 1.1 is the following:

Corollary 1.2. *Let M be a residually finite monoid and let A be a finite set. Then every subsemigroup of $\text{CA}(M, A)$ is residually finite.* \square

In [9], it was shown by Mal'cev that every finitely generated residually finite semigroup is Hopfian and has a residually finite monoid of endomorphisms. Combining Corollary 1.2 with these results of Mal'cev, we get the following.

Corollary 1.3. *Let M be a residually finite monoid and let A be a finite set. Then every finitely generated subsemigroup of $\text{CA}(M, A)$ is Hopfian.* \square

Corollary 1.4. *Let M be a residually finite monoid and let A be a finite set. Suppose that T is a finitely generated subsemigroup of $\text{CA}(M, A)$. Then the monoid $\text{End}(T)$ of endomorphisms of T is residually finite.* \square

The next section precises the terminology used and collects some background material. For the convenience of the reader, we have also included a proof of the results of Mal'cev mentioned above. The proof of Theorem 1.1 is given in the final section.

2. PRELIMINARIES

2.1. Semigroups and monoids. A *semigroup* is a set equipped with an associative binary operation. We shall use a multiplicative notation for the operation on semigroups. If S and T are semigroups, a *semigroup morphism* from S to T is a map $\varphi: S \rightarrow T$ such that $\varphi(s_1 s_2) = \varphi(s_1) \varphi(s_2)$ for all $s_1, s_2 \in S$. We denote by $\text{Mor}(S, T)$ the set consisting of all semigroup morphisms from S to T . A relation γ on a semigroup S is called a *congruence relation* if there exist a semigroup T and a semigroup morphism $\varphi: S \rightarrow T$ such that γ is the *kernel relation* associated with φ , i.e., the equivalence relation defined by

$$\gamma := \{(s_1, s_2) \in S \times S : \varphi(s_1) = \varphi(s_2)\}.$$

Equivalently, an equivalence relation $\gamma \subset S \times S$ on S is a congruence relation if and only if $(s_1, s_2) \in \gamma$ implies $(ss_1, ss_2) \in \gamma$ and $(s_1 s, s_2 s) \in \gamma$ for all $s, s_1, s_2 \in S$.

Suppose that γ is a congruence relation on a semigroup S . Then there is a natural semigroup structure on the quotient set S/γ . This semigroup structure is the only one for which the canonical map from S onto S/γ (i.e., the map sending each $s \in S$ to its γ -class $[s] \in S/\gamma$) is a semigroup morphism. Moreover, γ is the kernel relation associated with this semigroup morphism. One says that the congruence relation γ is of *finite index* if the quotient semigroup S/γ is finite.

A *monoid* is a semigroup admitting an identity element. The identity element of a monoid M is denoted 1_M . If M and N are monoids, a monoid morphism from M to N is a semigroup morphism from M to N that sends 1_M to 1_N . Suppose that γ is a congruence relation on a monoid M . Then the quotient semigroup M/γ is a monoid. Moreover, the canonical semigroup morphism from M onto M/γ is a monoid morphism.

2.2. Residually finite semigroups. It is clear from the general definition of residual finiteness given in the Introduction that a group is residually finite as a group if and only if it is residually finite as a monoid and that a monoid is residually finite as a monoid if and only if it is residually finite as a semigroup.

The class of residually finite semigroups includes all free groups and hence (since residual finiteness is a hereditary property) all free monoids and all free semigroups, all polycyclic groups [6] and hence all finitely generated nilpotent groups, all finitely generated commutative semigroups [10] (see also [7] and [2]), all finitely generated semigroups that are both regular in the sense of von Neumann and nilpotent in the sense of Mal'cev [8], and all finitely generated semigroups of matrices over commutative rings [9], [11].

The following two fundamental results about finitely generated residually finite semigroups are due to Mal'cev [9] (see also [4]).

Theorem 2.1 (Mal'cev). *Every finitely generated residually finite semigroup is Hopfian.*

Proof. Let S be a finitely generated residually finite semigroup. Suppose that $\psi: S \rightarrow S$ is a surjective endomorphism of S . Let s_1 and s_2 be distinct elements in S . Since S is residually finite, there exists a finite semigroup T and a semigroup morphism $\rho: S \rightarrow T$ such that $\rho(s_1) \neq \rho(s_2)$. Consider the map

$$\Phi: \text{Mor}(S, T) \rightarrow \text{Mor}(S, T)$$

defined by $\Phi(u) = u \circ \psi$ for all $u \in \text{Mor}(S, T)$. Observe that Φ is injective since ψ is surjective. On the other hand, as S is finitely generated and T is finite, the set $\text{Mor}(S, T)$ is finite. Therefore Φ is also surjective. In particular, there exists a morphism $u_0 \in \text{Mor}(S, T)$ such that $\rho = \Phi(u_0) = u_0 \circ \psi$. Since $\rho(s_1) \neq \rho(s_2)$, this implies that $\psi(s_1) \neq \psi(s_2)$. We deduce that ψ is injective. This shows that S is Hopfian. \square

Theorem 2.2 (Mal'cev). *Let S be a finitely generated residually finite semigroup. Then the monoid $\text{End}(S)$ is residually finite.*

Let us first establish the following auxiliary result.

Lemma 2.3. *Let S be a semigroup. Suppose that γ_1 and γ_2 are congruence relations of finite index on S . Then the congruence relation $\gamma := \gamma_1 \cap \gamma_2$ is also of finite index on S .*

Proof. Two elements in S are congruent modulo γ if and only if they are both congruent modulo γ_1 and modulo γ_2 . Therefore, there is an injective map from S/γ into $S/\gamma_1 \times S/\gamma_2$ given by $[s] \mapsto ([s]_1, [s]_2)$, where $[s]$ (resp. $[s]_1$, resp. $[s]_2$) denote the class of $s \in S$ modulo γ (resp. γ_1 , resp. γ_2). As the sets S/γ_1 and S/γ_2 are finite by our hypothesis, we deduce that S/γ is also finite, that is, γ is of finite index on S . \square

Proof of Theorem 2.2. Let $\alpha_1, \alpha_2 \in \text{End}(S)$ such that $\alpha_1 \neq \alpha_2$. Then we can find an element $s_0 \in S$ such that $\alpha_1(s_0) \neq \alpha_2(s_0)$. As S is residually finite, there exist a finite semigroup T and a semigroup morphism $\rho: S \rightarrow T$ satisfying $\rho(\alpha_1(s_0)) \neq \rho(\alpha_2(s_0))$. Consider the set $\gamma \subset S \times S$ defined by

$$\gamma := \bigcap_{\psi \in \text{Mor}(S, T)} \gamma_\psi,$$

where γ_ψ denotes the kernel congruence relation associated with the semigroup morphism $\psi: S \rightarrow T$. Observe first that γ is a congruence relation on S since it is the intersection of a family of congruence relations on S . On the other hand, for every $\alpha \in \text{End}(S)$ and $(s_1, s_2) \in \gamma$, we have that $(\alpha(s_1), \alpha(s_2)) \in \gamma$ since $\psi \circ \alpha \in \text{Mor}(S, T)$ for every $\psi \in \text{Mor}(S, T)$. We deduce that α induces an endomorphism $\bar{\alpha}$ of S/γ , given by $\bar{\alpha}([s]) = [\alpha(s)]$, for all $s \in S$ (here $[s]$ denotes the γ -class of s). The map $\alpha \mapsto \bar{\alpha}$ is clearly a morphism from $\text{End}(S)$ into $\text{End}(S/\gamma)$. Now the set $\text{Mor}(S, T)$ is finite since S is finitely generated and T is finite. Moreover, as the semigroup T is finite, the congruence relation γ_ψ is of finite index on S for every $\psi \in \text{Mor}(S, T)$. By applying Lemma 2.3, we deduce that the congruence relation γ is of finite index on S . Thus, the semigroup S/γ is finite and hence the monoid $\text{End}(S/\gamma)$ is also finite. On the other hand, we have that

$$\bar{\alpha}_1([s_0]) = [\alpha_1(s_0)] \neq [\alpha_2(s_0)] = \bar{\alpha}_2([s_0])$$

since $\gamma \subset \gamma_\rho$ and $\rho(\alpha_1(s_0)) \neq \rho(\alpha_2(s_0))$. Therefore $\bar{\alpha}_1 \neq \bar{\alpha}_2$. This shows that the monoid $\text{End}(S)$ is residually finite. \square

2.3. Shift spaces. Let A be a finite set, called the *alphabet*, and let M be a monoid. The set A^M , consisting of all maps $x: M \rightarrow A$, is called the set of *configurations* over the monoid M and the alphabet A . We equip A^M with its *prodiscrete topology*, i.e., the product topology obtained by taking the discrete topology on each factor A of $A^M = \prod_{m \in M} A$. Observe that A^M is a compact Hausdorff totally disconnected space since it is a product of compact Hausdorff totally disconnected spaces. We also equip A^M with the *M-shift*, that is, the action of the monoid M on A^M given by $(m, x) \mapsto mx$, where

$$mx(m') = x(m'm)$$

for all $x \in A^M$ and $m, m' \in M$.

Let γ be a congruence relation on M . We define the subset $\text{Inv}(\gamma) \subset A^M$ by

$$\text{Inv}(\gamma) := \{x \in A^M : m_1x = m_2x \text{ for all } (m_1, m_2) \in \gamma\}.$$

Observe that $\text{Inv}(\gamma)$ is *M-invariant*, i.e., $mx \in \text{Inv}(\gamma)$ for all $m \in M$ and $x \in \text{Inv}(\gamma)$. One immediately checks that $\text{Inv}(\gamma)$ consists of all configurations $x \in A^M$ that are constant on each γ -class. This implies in particular that the set $\text{Inv}(\gamma)$ is finite whenever γ is of finite index.

A configuration $x \in A^M$ is called *periodic* if its orbit

$$Mx := \{mx : m \in M\}$$

is finite.

Residually finite monoids are characterised by the density of periodic configurations in their shift spaces. More precisely, we have the following result (see [3, Proposition 2.14]).

Theorem 2.4. *Let M be a monoid and let A be a finite set with more than one element. Then the following conditions are equivalent:*

- (a) *the monoid M is residually finite;*
- (b) *the set of periodic configurations of A^M is dense in A^M for the prodiscrete topology.*

□

2.4. Cellular automata. Let M be a monoid and let A be a finite set. A *cellular automaton* over the monoid M and the alphabet A is a map $\tau: A^M \rightarrow A^M$ that is continuous for the prodiscrete topology on A^M and commutes with the shift action, i.e., satisfies $\tau(mx) = m\tau(x)$ for all $m \in M$ and $x \in A^M$. We denote by $\text{CA}(M, A)$ the set consisting of all cellular automata $\tau: A^M \rightarrow A^M$. It is clear from the above definition that $\text{CA}(M, A)$ is a monoid for the composition of maps.

Example 2.5. If $m \in M$, one immediately checks that the map $\tau_m: A^M \rightarrow A^M$, defined by $\tau_m(x) = x \circ L_m$ for all $x \in A^M$, where $L_m: M \rightarrow M$ denotes the left-multiplication by m , is a cellular automaton. Moreover, the map $m \rightarrow \tau_m$ yields an anti-monoid morphism from M into $\text{CA}(M, A)$. This means that τ_{1_M} is the identity map on A^M and that $\tau_{m_1 m_2} = \tau_{m_2} \circ \tau_{m_1}$ for all $m_1, m_2 \in M$. This monoid anti-morphism is injective as soon as the alphabet A has more than one element. Indeed, let $m_1, m_2 \in M$ with $m_1 \neq m_2$. Suppose that a and b are distinct elements in A and consider the configuration $x \in A^M$ defined by $x(m_1) = a$ and $x(m) = b$ for all $m \in M \setminus \{m_1\}$. We then have $\tau_{m_1}(x) \neq \tau_{m_2}(x)$ since

$$\tau_{m_1}(x)(1_M) = x(m_1) = a \neq b = x(m_2) = \tau_{m_2}(x)(1_M),$$

and hence $\tau_{m_1} \neq \tau_{m_2}$.

3. PROOF OF THE MAIN RESULT

In this section, we give the proof of Theorem 1.1.

Proof of (a) \Rightarrow (b). Suppose that M is residually finite. Let $\tau_1, \tau_2 \in \text{CA}(M, A)$ be two distinct cellular automata.

Since M is residually finite, the periodic configurations in A^M are dense in A^M (see Theorem 2.4). As τ_1 and τ_2 are continuous and A^M is Hausdorff, this implies that there exists a periodic configuration $x_0 \in A^M$ such that $\tau_1(x_0) \neq \tau_2(x_0)$. Consider the orbit $Y := Mx_0$ of x_0 under the M -shift. As the set Y is M -invariant, the equivalence relation γ defined by

$$\gamma := \{(m_1, m_2) \in M \times M : m_1 y = m_2 y \text{ for all } y \in Y\} \subset M \times M$$

is a congruence relation on M . Moreover, γ is of finite index since Y is finite. Consider now the associated M -invariant subset

$$X := \text{Inv}(\gamma) = \{x \in A^M : m_1 x = m_2 x \text{ for all } (m_1, m_2) \in \gamma\} \subset A^M.$$

Note that X is finite since the congruence relation γ is of finite index. As every cellular automaton $\tau \in \text{CA}(M, A)$ is M -equivariant, restriction to X yields a monoid morphism $\rho: \text{CA}(M, A) \rightarrow \text{Map}(X)$, where $\text{Map}(X)$ denotes the *symmetric monoid* of X , i.e., the set consisting of all maps $f: X \rightarrow X$ with the composition of maps as the monoid operation. Observe that the monoid $\text{Map}(X)$ is finite since X is finite. On the other hand, as $x_0 \in Y \subset X$ and $\tau_1(x_0) \neq \tau_2(x_0)$, we have that $\rho(\tau_1) \neq \rho(\tau_2)$. This shows that $\text{CA}(M, A)$ is residually finite. □

Proof of (b) \Rightarrow (a). First observe that a semigroup is residually finite if and only if its opposite semigroup is (this trivially follows from the fact that a semigroup is finite if and only if its opposite semigroup is). Suppose now that the monoid $CA(M, A)$ is residually finite. Since there is an injective monoid anti-morphism $M \rightarrow CA(M, A)$ (see Example 2.5) and residual finiteness is hereditary, we deduce that the opposite monoid of M is residually finite. By the above observation, the monoid M is itself residually finite. \square

Remark 3.1. Let us observe that Corollary 1.3 and Corollary 1.4 become false if we drop the hypothesis that the subsemigroup of $CA(M, A)$ is finitely generated, even if we restrict to the case where M is the group \mathbb{Z} of integers (the classical case studied in symbolic dynamics). Indeed, let A be a finite set with more than one element. It can be shown, using the technique of *markers* introduced in [5], that the free group on two generators can be embedded in $CA(\mathbb{Z}, A)$ (see [1, Theorem 2.4] for a more general statement). It follows that the free group F_∞ on infinitely many generators g_i , $i \in \mathbb{N}$, can be also embedded in $CA(\mathbb{Z}, A)$. Now, the group F_∞ is not Hopfian since the unique endomorphism $\psi \in \text{End}(F_\infty)$ satisfying $\psi(g_i) = g_{i-1}$ if $i \geq 1$ and $\psi(g_0) = g_0$ is clearly surjective but not injective. On the other hand, by using automorphisms of F_∞ induced by permutations of its generators, one sees that the automorphism group of F_∞ contains a copy of the symmetric group $\text{Sym}(\mathbb{N})$ (the group of permutations of \mathbb{N}). The group $\text{Sym}(\mathbb{N})$ is not residually finite since, by Cayley's theorem, every countable group can be embedded in $\text{Sym}(\mathbb{N})$ and there exist countable groups that are not residually finite (e.g., the additive group \mathbb{Q} of rational numbers or the Baumslag-Solitar group $BS(2, 3) := \langle a, b : ba^2b^{-1} = a^3 \rangle$). Therefore, the monoid $\text{End}(F_\infty)$ is not residually finite either.

REFERENCES

- [1] M. BOYLE, D. LIND, AND D. RUDOLPH, *The automorphism group of a shift of finite type*, Trans. Amer. Math. Soc., 306 (1988), pp. 71–114.
- [2] W. H. CARLISLE, *Residual finiteness of finitely generated commutative semigroups*, Pacific J. Math., 36 (1971), pp. 99–101.
- [3] T. CECCHERINI-SILBERSTEIN AND M. COORNAERT, *On surjunctive monoids*, arXiv:1409.1340.
- [4] T. EVANS, *Residually finite semigroups of endomorphisms*, J. London Math. Soc. (2), 2 (1970), pp. 719–721.
- [5] G. A. HEDLUND, *Endomorphisms and automorphisms of the shift dynamical system*, Math. Systems Theory, 3 (1969), pp. 320–375.
- [6] K. A. HIRSCH, *On infinite soluble groups. III*, Proc. London Math. Soc. (2), 49 (1946), pp. 184–194.
- [7] G. LALLEMENT, *On a theorem of Malcev*, Proc. Amer. Math. Soc., 30 (1971), pp. 49–54.
- [8] ———, *On nilpotency and residual finiteness in semigroups*, Pacific J. Math., 42 (1972), pp. 693–700.
- [9] A. I. MAL'CEV, *On isomorphic matrix representations of infinite groups*, Rec. Math. [Mat. Sbornik] N.S., 8 (50) (1940), pp. 405–422.
- [10] ———, *On homomorphisms onto finite groups*, Ivanov. Gos. Ped. Inst. U?. Zap., (1958), pp. 49–60.
- [11] J. R. STALLINGS, *Notes for math 257, geometric group theory, fall semester 2000 at uc berkeley*, <http://math.berkeley.edu/~stall/math257>.
- [12] K. VARADARAJAN, *Some recent results on Hopficity, co-Hopficity and related properties*, in International Symposium on Ring Theory (Kyongju, 1999), Trends Math., Birkhäuser Boston, Boston, MA, 2001, pp. 371–392.

DIPARTIMENTO DI INGEGNERIA, UNIVERSITÀ DEL SANNIO, C.SO GARIBALDI 107, 82100 BENEVENTO, ITALY

E-mail address: `tceccher@mat.uniroma3.it`

INSTITUT DE RECHERCHE MATHÉMATIQUE AVANCÉE, UMR 7501, UNIVERSITÉ DE STRASBOURG ET CNRS, 7 RUE RENÉ-DESCARTES, 67000 STRASBOURG, FRANCE

E-mail address: `coornaert@math.unistra.fr`